enDERWENT ENHANCED ENGLISH-LANGUAGE ABSTRACT FOR

RU 2067313

Subaccount is set to 17299-008002

16/3,AB/1

011246909
WPI Acc No: 1997-224812/ **199720**
XRPX Acc No: N97-186049

Personal computer data access protection unit - Forms functionally closed logical medium for each user to protect against unauthorised access

Patent Assignee: AUTOM DES SYSTEMS CONSTR BUR (AUTO-R); INFOKRIPT CO LTD (INFO-R)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
RU 2067313	C1	19960927	RU 95104292	A	19950329	199720	B

Priority Applications (No Type Date): RU 95104292 A 19950329
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
RU 2067313	C1		6	G06F-012/14	

Abstract (Basic): RU 2067313 C

Protection unit comprises a ROM, personal computer data exchange controller, external data carrier data exchange controller and a removable contact set for reading data from the external carrier. The ROM input-outputs and computer data exchange controller are for connecting to the computer.

USE - Protection unit concerns means of protecting data and comprises external data carrier made in form of volatile memory, into which are written personal data on user and hash functions of all protected files for given user.

Dwg.1/2

(19) **RU** (11) **2 067 313** (13) **C1**

(51) МПК[6] **G 06 F 12/14**

РОССИЙСКОЕ АГЕНТСТВО
ПО ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ РОССИЙСКОЙ ФЕДЕРАЦИИ

(21), (22) Заявка: 95104292/09, 29.03.1995

(46) Дата публикации: 27.09.1996

(56) Ссылки: Спесивцев А.В. и др. Защита информации в персональных ЭВМ. - М.: Радио и связь, 1992, с.25 - 26.

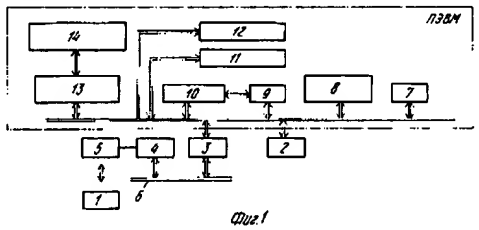
(71) Заявитель:
Акционерное общество закрытого типа "Особое конструкторское бюро систем автоматизированного проектирования", Товарищество с ограниченной ответственностью "Фирма ИНФОКРИПТ"

(73) Патентообладатель:
Акционерное общество закрытого типа "Особое конструкторское бюро систем автоматизированного проектирования", Товарищество с ограниченной ответственностью "Фирма ИНФОКРИПТ"

(54) УСТРОЙСТВО ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ, ХРАНИМОЙ В ПЕРСОНАЛЬНОЙ ЭВМ

(57) Реферат:

Изобретение относится к средствам защиты информации и содержит внешний носитель информации, выполненный в виде энергонезависимой памяти, в которую записана персональная информация о пользователе и хэш-функция всех защищаемых файлов данного пользователя. Устройство содержит также постоянное запоминающее устройство, контроллер обмена информацией с ПЭВМ, контроллер обмена информацией с внешним носителем информации и выносной контактный узел считывания информации с внешнего носителя. Для подключения к ПЭВМ служат входы/выходы ПЗУ и контроллера обмена информацией с ПЭВМ. Устройство обеспечивает создание функционально-замкнутой логической среды, определенной для каждого пользователя ПЭВМ, что повышает надежность защиты информации, хранимой в ПЭВМ, от несанкционированного доступа. 2 ил.



Фиг.1

RU 2067313 C1

RU 2067313 C1

(19) **RU** (11) **2 067 313** (13) **C1**

(51) Int. Cl.[6] **G 06 F 12/14**

RUSSIAN AGENCY
FOR PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: **95104292/09, 29.03.1995**

(46) Date of publication: **27.09.1996**

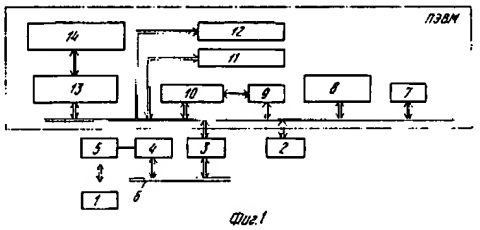
(71) Applicant:
Aktsionernoe obshchestvo zakrytogo tipa "Osoboe konstruktorskoe bjuro sistem avtomatizirovannogo proektirovanija", Tovarishchestvo s ogranichennoj otvetstvennost'ju "Firma INFOKRIPT"

(73) Proprietor:
Aktsionernoe obshchestvo zakrytogo tipa "Osoboe konstruktorskoe bjuro sistem avtomatizirovannogo proektirovanija", Tovarishchestvo s ogranichennoj otvetstvennost'ju "Firma INFOKRIPT"

(54) DEVICE FOR PROTECTION AGAINST UNAUTHORIZED ACCESS TO INFORMATION THAT IS STORED IN PERSONAL COMPUTER

(57) Abstract:

FIELD: computer engineering, information security. SUBSTANCE: device has external information storage unit which is designed as power- independent memory, where personal information about user and hash information about all protected files of this user are stored. In addition device has read-only memory unit, controller for interface to computer, controller fro interface to external storage unit, remote contact unit for reading information from external storage unit. For connection to computer inputs and outputs of read-only memory unit and of computer interface controller are used. Device provides closed functionality environment for all users of computer. EFFECT: increased reliability of information protection against unauthorized access. 2 dwg



Фиг.1

RU 2067313 C1

RU 2067313 C1

Изобретение относится к защите информации, а более точно к устройству защиты от несанкционированного доступа к информации, хранимой в персональной ЭВМ, и может быть использовано в автоматизированных системах на базе персональных ЭВМ для защиты информации и ресурсов персональных ЭВМ от несанкционированного доступа.

Использование современных информационных технологий при необходимости обеспечения конфиденциальности хранения и обработки данных является источником возникновения специфических угроз со стороны злоумышленников. С этим связана необходимость применения специальных средств защиты информационных систем от несанкционированного доступа (НСД). Штатные средства защиты персональных ЭВМ (ПЭВМ) от НСД, например, использование паролей пользователей, устанавливаемых с помощью документации к поставляемым ПЭВМ, гарантированно не решает данную задачу, так как имеется возможность отключить систему контроля путем принудительного разряда питающей батареи.

Известны и более сложные способы обхода штатных средств защиты ПЭВМ от НСД. Так, например, если доступ к компьютеру не контролируется, вполне вероятно, что однажды после вызова обычно используемой программы и ввода пароля компьютер "зависнет". Обычно это не вызывает никаких подозрений и воспринимается как проявление ненадежности техники. После перегрузки компьютера, повторного вызова программы и ввода пароля система работает как обычно. Но при этом не исключено, что в первый раз загружалась вовсе не требуемая программа, а специальная программа "перехватчик паролей", и пароль уже не является секретным он дискредитирован "перехватчиком паролей". Таким образом, необходимым элементом обеспечения информационной безопасности является специальная технология сохранения в тайне ключевой информации.

Обычно для контроля целостности программного обеспечения и хранимых данных используются программы типа известной программы ADINF, которая вычисляет контрольную сумму файлов. Для защиты информации от угрозы ее несанкционированного зменения с сохранением прежнего значения контрольной суммы необходимо применять специально разработанные алгоритмы вычисления контрольных сумм файлов, называемые алгоритмами хэширования информации. Хэш-функция (контрольная сумма, вычисленная по алгоритму хэширования) обладает тем свойством, что для любого заданного блока данных,имеющего заданное значение хэш-функции, практически невозможно в реальное время подобрать другой блок данных, имеющий то же значение хэш-функции.

Таким образом, контроль целостности программ и данных на компьютере с помощью программных свойств, размещенных на этом те компьютере и также требующих проверки на собственную целостность перед их запуском, однозначно не достигает поставленной цели.

К известным системам создания изолированной программной среды можно отнести систему, описанную в разработке Unvisible Disk фирмы ЛАН Крипто (А. Щербаков, Разрушающие программные воздействия. М. ЭДЕЛЬ, 1993).

Суть данной разработки состоит в том, что загрузка дисковой операционной системы (DOS) производится с охраняемого от несанкционированного доступа гибкого диска, после чего уже могут быть использованы другие системы защиты от НСД, не имеющие возможностей по контролю над целостностью общих системных ресурсов ПЭВМ. Обеспечивая принципиальную возможность создания в комплексе с дополнительными системами защиты хранимых на ПЭВМ данных от НСД достаточно надежной защиты информации, описанная система реализации изолированной программной среды малопригодна по двум обстоятельствам.

Первое потенциальному злоумышленнику оставляется возможность в отсутствии контроля за доступом к ПЭВМ включать ПЭВМ, загружать системные и запускать собственные программные модули с гибкого диска, внося программные закладки, под которыми понимается несанкционированно записанная на жесткий диск ПЭВМ программа, запуск которой разрушает систему защиты ПЭВМ от НСД. Зарегистрированные пользователи, имеющие намерение осуществить несанкционированный доступ к чужим ресурсам и данным, имеют в данном случае полную свободу действий.

Второе возникают определенные неудобства в работе легальных пользователей, вытекающие из необходимости использовать специально охраняемую в режимном органе учреждения проверенную системную дискету, необходимость дополнительных организационно-технических мер для верификации данной дискеты при передаче ее из рук в руки.

Наиболее близким к изобретению является устройство защиты от несанкционированного доступа к информации, хранимой в персональной ЭВМ, содержащее внешний носитель информации и расположенные на общей плате постоянное запоминающее устройство (ПЗУ) и контроллер обмена информацией с персональной ЭВМ, входы/выходы которых предназначены для подключения к персональной ЭВМ [см.источник]

В качестве внешнего носителя информации в известной разработке использована дискета, содержащая криптографические ключи запрашиваемых данных. На общей плате устройства KRYPTON также размещены два 32-разрядных однокристальных процессора, осуществляющие шифрование в соответствии со стандартом шифрования и подключенные к общей шине управления и обмена данными с ПЭВМ.

На жесткий диск ПЭВМ предварительно записано необходимое программное обеспечение, поддерживающее интерфейс обмена данными между BIOS (basic input/ouput System) ПЭВМ и процессорами платы RYPTON. Данное программное

RU 2067313 C1

RU 2067313 C1

обеспечение вместе с другими указанными ресурсами поддерживает функции разграничения доступа к компьютеру и логическим дискам жесткого диска ПЭВМ. Устройство осуществляет "прозрачное" шифрование данных на жестком диске. Суть режима "прозрачного" шифрования состоит в том, что всякое обращение к жесткому диску средствами базовой системы ввода/ вывода BIOS приводит к шифрованию/расшифрованию данных. Программное обеспечение, поддерживающее интерфейс обмена данными между BIOS ПЭВМ и процессорами платы KRYPTON переносится с жесткого диска в ОЗУ ЛЭВМ во время загрузки компьютера (до загрузки дисковой операционной системы DOS) и становится составной частью расширенной системы BOS для доступа к данным на жестком диске ПЭВМ. При этом обеспечивается полное шифрование логических дисков жесткого диска, что предотвращает появление "секретного остатка" данных. Разграничение доступа к хранимой в зашифрованном виде информации реализовано посредством предъявления дискеты, содержащей криптографические ключи запрашиваемых данных.

Данное устройство обеспечивает разграничение доступа к "персональным" данным, сохраняемым под персональными ключами шифрования, однако общие ресурсы пользователей при таком подходе к созданию системы защиты ПЭВМ от НСД оказываются доступными всем зарегистрированным пользователям и в силу этого полностью отсутствует возможность разграничения доступа пользователей, например, к системным ресурсам, которые не могут шифроваться различными ключами. В силу этого обстоятельства зарегистрированные пользователи системы, имеющие злоумышленные намерения, получают возможность внедрения в систему специальных программных закладок. Программные "закладки" могут выполнять самые различные действия, в том числе перехватывать конфиденциальные данные после их расшифрования и сохранять их в ПЭВМ "до востребования".

Чтобы воспрепятствовать внедрению в систему программных закладок со стороны зарегистрированных пользователей, необходимо иметь средства создания изолированной от внешнего вмешательства программной среды или среды, проверенной на отсутствие программных закладок к моменту запуска прикладных программ.

Возможным вариантом решения проблемы является создание для каждого пользователя собственной функционально замкнутой среды. Здесь имеется в виду, что каждому лицу, имеющему право доступа к компьютеру, предоставляется возможность пользовать только назначенные ему программы. Система защиты технически не должна давать возможность пользователю выполнять неназначенные ему программы, а расширение прав доступа может быть реализовано только администратором.

Упомянутый и описанный выше комплекс KRYPTON данными возможностями не обладает. Кроме того, регулярно выполняемые операции шифрования/расшифрования занимают у ПЭВМ определенный ресурс вычислительной мощности, вносят заметную задержку в реакцию машины на команды оператора, что отрицательно сказывается на эргономических характеристиках рабочего места.

Целью изобретения является создание устройства защиты от несанкционированного доступа к информации, хранимой в персональной ЭВМ, за счет конструктивного выполнения которого достигалась бы возможность создания функциональнозамкнутой программно-логической среды, определенной для каждого пользования ПЭВМ, что обеспечивало бы доступ к ресурсам ПЭВМ и хранимой в ПЭВМ информации только зарегистрированным пользователям, создавая надежную защиту от несанкционированного доступа.

Это достигается тем, что в устройство защиты от несанкционированного доступа к информации, хранимой в персональной ЭВМ, содержащее внешний носитель информации, и расположенные на общей плате постоянное запоминающее устройство и контроллер обмена информацией с персональной ЭВМ, выходы которых предназначены для подключения к персональной ЭВМ введены контроллер обмена информацией с внешним носителем информации, расположенный на общей плате устройства, и выносной контактный узел считывания информации с внешнего носителя информации, выходом подключенный ко входу контроллера обмена информацией с внешним носителем информации, причем внешний носитель информации выполнен в виде энергонезависимой памяти, в которую записана персональная идентификационная информация о пользователе и хэш-функция всех защищаемых файлов данного пользователя, а а постоянное запоминающее устройство предназначено для хранения кодов контроля целостности информации персональной ЭВМ и кодов считывания информации с внешнего носителя информации, при этом входы/выходы контроллера обмена информацией с внешним носителем информации через магистрали локальной шины устройства соединены со входами/выходами контроллера обмена информацией с персональной ЭВМ.

Отличительной особенностью изобретения является то, что в нем используется внешний носитель информации, содержащий индивидуальную неизменяемую для каждого пользователя ПЭВМ информацию, а именно его персональный идентификатор в виде энергонезависимой памяти, в которую записана персональная идентификационная информация о пользователе и вычисленное значение хэш-функции защищаемых от изменений файлов. Пароль пользователя, список защищаемых от изменений файлов, вычисленное значение их хэш-функций, имя назначенной пользователю стартовой программы и список разрешенных к выполнению программ записаны на жесткий диск ПЭВМ.

Введение в устройство контроллера обмена информацией с внешним носителем информации и выносного контактного узла считывания информации в сочетании с

RU 2067313 C1

RU 2067313 C1

использованием постоянного запоминающего устройства, хранящего коды контроля целостности информации ПЭВМ и коды считывания информации с внешнего носителя информации, позволяют создать функционально-замкнутую программно-логическую среду, обеспечивая эффективную защиту информации, хранящейся в ПЭВМ, от несанкционированного доступа.

Устройство компактно и устанавливается при эксплуатации в свободный слот ПЭВМ. Используемый внешний носитель информации в отличие дискеты, применяемой в известной системе, труднокопируем, отличается быстродействием, с него могут быть осуществлены запись и считывание информации. Кроме того, такой носитель информации имеет небольшие массо-габаритные характеристики.

Устройство защиты от несанкционированного доступа информации, хранимой в персональной ЭВМ, технологически может быть легко реализовано на производстве, так как не содержит каких-либо сложных электронных блоков.

В дальнейшем изобретение поясняется описанием конкретного варианта его выполнения и прилагаемыми чертежами, на которых на фиг.1 изображена блок-схема устройства защиты от несанкционированного доступа к информации, хранимой в персональной ЭВМ, подключенного к ПЭВМ, согласно изобретению; на фиг. 2 функциональная схема, поясняющая работу устройства.

Устройство защиты от несанкционированного доступа к информации, хранимой в ПЭВМ, содержит внешний носитель 1 информации и расположенные на общей плате постоянное запоминающее устройство (ПЗУ) 2, в котором хранятся коды считывания информации с внешнего носителя 1 информации и коды контроля целостности информации ПЭВМ, контроллер 3 обмена информацией с персональной ЭВМ и контроллер 4 обмена информацией с внешним носителем информации. С контроллером 4 электрически связан выносной контактный узел 5 считывания информации с внешнего носителя информации. Плата с расположенными на ней ПЗУ 2 и контроллерами 3,4 устанавливается в свободный слот ПЭВМ и подключается через соответствующие входы/выходы к общей шине управления и обмена данными с ПЭВМ (как это изображено на чертеже), при этом выносной контактный узел 5 закрепляется на внешней панели ПЭВМ. Входы/выходы контроллера 4 обмена информацией с внешним носителем информации соединены через магистрали локальной шины 6 устройства со входами/выходами контроллера 3.

Для пояснения взаимодействия патентуемого устройства с ПЭВМ на чертеже представлены ее основные функциональные узлы: ПЗУ 7, содержащее BIOS, жесткий диск 8, с записанными на нем DOS, прикладными программами и регистрационными данными, ОЗУ 9, процессор 10, клавиатура 11, дискет 12, дисковод 13 гибкого диска и гибкий диск 14 (дискета пользователя).

В устройстве внешний носитель 1 информации выполнен в виде энергонезависимой памяти, в которую записана персональная идентификационная информация о пользователе и хэшфункция всех защищаемых файлов данного пользователя. В качестве такого носителя 1 информации может быть использован идентификатор семейства Touch Memory (ТМ).

Внешний носитель 1 информации М размещен в металлическом корпусе с одним сигнальным контактом и одним контактом земли. Корпус диаметра 15 и толщиной 5 мм, напоминающий миниатюрную пуговичную батарейку, крепится на изделии либо на носителе. Информация записывается и считывается простым касанием считывающего устройства, расположенного на корпусе ТМ.

Благодаря своему конструктивному выполнению ТМ имеет высокую надежность, а уникальность достигается за счет присвоения заводом-изготовителем уникального кода (64 бита). По сравнению с известным персональным идентификатором chip-картой ТМ примерно в 10 раз дешевле. Объем памяти ТМ достигает 4 Кбит, а скорость обмена данными 16,6 КВ/с.

Таким образом, по габаритным характеристикам, по надежности, по цене, по быстродействию и по степени защиты от копирования устройство Touch Memory имеет оптимальные совокупные характеристики по отношению к другим носителям информации.

В изобретении применены стандартные контроллеры 3,4 обмена информацией, адаптированные по электрическим параметрам для обмена данными с внешним носителем информации ТМ и персональной ЭВМ. Подобные контроллеры широко известны и описаны.

Применяемый в описываемом устройстве внешний контактный узел 5 считывания информации широко известен в подобных устройствах и может представлять собой пару контактов, концентрично расположенных, разделенных слоем диэлектрика и соединенных проводами с платой устройства.

Перед началом эксплуатации ПЭВМ с установленной системой защиты с помощью программного обеспечения системы защиты ПЭВМ от НСД в регистрационные файлы на жестком диске 8 (фиг. 1) ПЭВМ записывают переменные параметры контрольную информацию, которая определяет права доступа пользователей к ресурсам ПЭВМ: пароль пользователя, список защищаемых от изменений файлов и имя стартовой программы для данного пользователя, а на внешний носитель 1 информации ТМ записывают вычисленное значение хэш-функции защищаемых от изменений файлов.

Устройство защиты от несанкционированного доступа к информации, хранимой в персональной ЭВМ, после установки в компьютер, работает следующим образом.

При включении ПЭВМ управление ее загрузкой вначале осуществляется в штатном режиме, но до окончания этапа загрузки BIOS программа, записанная в ПЗУ 2 (фиг. 1), перехватывает управление начальной загрузкой ПЭВМ на том этапе, на котором уже возможно выполнять операции чтения/ записи

RU 2067313 C1

RU 2067313 C1

информации по секторам дорожек жесткого диска в ПЭВМ, но до начала загрузки DOS (фиг. 2).

После перехвата управления начальной загрузкой ПЭВМ на себя программа, записанная в ПЗУ 2, выдает на дисплей 12 ПЭВМ приглашение пользователю прикоснуться своим носителем 1 информации ТМ к выносному контактному узлу 5 считывания информации и считывает с носителя 1 информации ТМ его регистрационный номер и записанное в ней значение хэшфункции (контрольную сумму) всех файлов, занесенных в регистрационный список защищаемых файлов для данного пользователя; затем, если предъявленный носитель 1 информации ТМ зарегистрирован в регистрационном файле на жестком диске 8 ПЭВМ, программа выполняет дальнейшие действия, в противном случае выдает на дисплей 12 предупреждение и повторное приглашение.

Программа, записанная в ПЗУ 2. выдает затем на дисплей 12 приглашение пользователю ввести свой пароль с клавиатуры 11; затем, если введенный пароль совпал с хранимым в регистрационном файле на жестком диске 8 ПЭВМ, программа выполняет дальнейшие действия, в противном случае выдает на дисплей 12 предупреждение и повторное приглашение.

Затем программа, записанная в ПЗУ 2, вычисляет значение хэш-функции всех файлов, занесенных в список защищаемых для данного пользователя и сравнивает полученное значение с ранее прочитанной записью на носителе 1 информации ТМ; при совпадении вычисленного значения с хранимым в носителе 1 информации ТМ программа выполняет дальнейшие действия, при несовпадении требует вмешательства администратора.

Далее программа, записанная в ПЗУ 2, блокирует возможность загрузки дисковой операционной системы DOS с гибкого диска 14.

После этого записанная в ПЗУ 2 программа передает управление штатным программно-аппаратным средствам ПЭВМ для завершения загрузки DIOS, загрузки DOS с жесткого диска 8 и выполнения модифицированных системных файлов CONFIG.SYS и AUTOEXEC.BAT.

Модификация системных файлов CONFIG. SYS и AUTOEXEC. BAT производится таким образом, что на время их выполнения блокируется клавиатура 11, а в результате их выполнения запускается резидентный программный модуль, контролирующий права пользователя на запуск различных программ в соответствии с регистрационными данными пользователя, записанными на жесткий диск 8, и стартовая для данного пользователя программа.

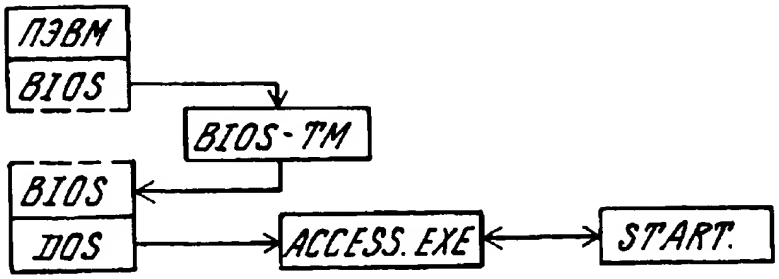
Таким образом, предлагаемое устройство защиты от несанкционированного доступа к информации, хранимой в ПЭВМ, позволяет реализовать контроль за доступом к ПЭВМ только зарегистрированных пользователей, разграничить их права доступа к исполняемым программным модулям и обеспечить контроль целостности хранимой в ПЭВМ информации.

Формула изобретения:

Устройство защиты от несанкционированного доступа к информации, хранимой в персональной ЭВМ, содержащее внешний носитель информации и расположенные на общей плате постоянное запоминающее устройство и контролер обмена информацией с персональной ЭВМ, выходы которых предназначены для подключения к персональной ЭВМ, отличающееся тем, что в него введены контролер обмена информацией с внешним носителем информации, расположенный на общей плате устройства, и выносной контактный узел считывания информации с внешнего носителя информации, выходом подключенный к входу контролера обмена информацией с внешним носителем информации, причем внешний носитель информации выполнен в виде энергонезависимой памяти, в которую записана первоначальная идентификационная информация о пользователе и хэш-функция всех защищаемых файлов данного пользователя, а постоянное запоминающее устройство предназначено для хранения кодов контроля целостности информации персональной ЭВМ и кодов считывания информации с внешнего носителя информации, при этом входы/выходы контролера обмена информацией с внешним носителем информации через магистрали локальной шины устройства соединены с входами/выходами контролера обмена информацией с персональной ЭВМ.

RU 2067313 C1

RU 2067313 C1



Фиг.2

RU 2067313 C1

RU 2067313 C1